SAND2008-3696C

A Resource Point-based Design Basis Threat:
A Concept for Reform of the DOE DBT

Andrew Walter
Strategic Studies Department, Sandia National Laboratories
P.O. Box 5800, MS-0839, Albuquerque NM, 87185-0839

SAND2008-XXXXC

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

ABSTRACT

The U.S. Department of Energy's (DOE) Design Basis Threat (DBT) is the fundamental policy that drives the safeguards and security programs at DOE and National Nuclear Security Administration (NNSA) facilities. Criticisms have long been raised by security professionals within the DOE/NNSA community that the DBT results in extremely sophisticated adversary attack scenarios that are highly incredible. Many scenarios possible under the current DBT result in large numbers of adversary personnel attacking DOE/NNSA facilities using multiple very advanced capabilities, weapons, and tactics. It has been argued that these extreme scenarios are unsupported by both analysis of past terrorist attacks and projections of potential future attacks.

A concept is offered to fundamentally alter the way the DOE DBT policy is derived and applied. First, a list of the resources and capabilities utilized by adversaries in historical terrorist attacks is coupled with projections of terrorists' potential out-year capabilities. Then, this list is examined by a group of experts to determine the relative "resource point value" of each capability/resource available to the adversary. These resource point values are relative values factoring in the perceived difficulty for an adversary to acquire/develop, field, deploy, and successfully utilize that capability within the continental United States. Using this list of values, the "total resource point value" of the historical terrorist attacks can be determined. Finally, based on this analysis of the total resources applied by terrorists to past attacks, "resource point caps" are assigned to DOE/NNSA sites; security analysts then design attack scenarios utilizing resources from the list whose cumulative resource point value does not exceed the resource point cap assigned for their site.

The proposed DBT method offers several advantages: it does not allow multiple advanced adversary capabilities to be used in a single scenario; it allows the use of large numbers of adversary personnel but at the cost of those personnel being extremely limited in capability; it continues to allow a "graded" approach to threat assignment; and it better captures the adversary's risk of pre-attack detection when they attempt to utilize advanced resources and capabilities.

INTRODUCTION & BACKGROUND

The fundamental policy that drives the safeguards and security programs at all U.S. Department of Energy (DOE) and National Nuclear Security Administration (NNSA) facilities is the DOE Design Basis Threat (DBT). Among other functions, the DBT policy stipulates the type

of threats each facility must defend against, the number of adversary personnel that must be defended against in an attack, and the weapons, capabilities, and tactics attackers might use. The DBT is reviewed annually by DOE and revised when threat projections or risk management actions require significant changes. While intended to be a long-term planning tool more than a reflection of dynamic real world threats, the DBT—through the attack scenarios created under it—drives security programs, plans, tactics, upgrades, and expenditures across the DOE/NNSA complex.

For the past several iterations of the DBT policy, many security professionals within the DOE/NNSA community have criticized the attack scenarios that result from its application. Many scenarios possible under the current DBT result in large numbers of adversary personnel attacking DOE/NNSA facilities using multiple very advanced capabilities, weapons, and tactics. While perhaps no individual adversary attribute listed in the DBT is extreme, the combination of many or all of the attributes into a single scenario (as allowed by the current DBT policy) results in scenarios that strain credibility and appear unsupported by both analysis of past terrorist attacks and projections of potential future attacks.

OVERVIEW OF THE PROPOSED APPROACH

To alleviate these concerns, a method is proposed to modify the way in which DOE establishes and applies its threat policy. Rather than listing all of the weapons, equipment, vehicles, and personnel (hereafter collectively referred to as "capabilities") an adversary might utilize in an attack on a DOE/NNSA facility and requiring the site to protect against attacks that utilize any or all of the capabilities simultaneously, the proposed approach will limit the combinations of capabilities based upon their sophistication. This is accomplished by assigning each separate capability a relative "resource point" value based upon its sophistication level. The sum of all of the resource point values for each individual adversary capability applied for an attack is the "total resource point value" for that attack scenario—and is indicative of the overall sophistication of the attack scenario.

By assigning a "resource point cap" to its facilities through a resource point-based DBT policy, DOE can effectively impose a clear ceiling on the adversary sophistication level it is requiring its facilities to protect against. This would be a departure from current DBT threat policy, where no clear line exists and attack scenario sophistication level can be nearly unlimited. With the resource point-based DBT policy described in this paper, communication regarding security analysis scenario sophistication is enhanced throughout the DOE/NNSA complex, facility security personnel and oversight organizations are held to clearly defined standards, and communication to Congress and other decision-makers regarding the level of protection provided by DOE to its national security assets is enhanced.

DETAILS OF IMPLEMENTING THE PROPOSED APPROACH

The following steps describe the process to create and implement a resource point-based DBT for DOE:

1. **Compilation of a list of all adversary capabilities (including trained personnel, weapons, equipment, vehicles, etc.) that might be used by DOE adversaries.** This list would be based on analysis of capabilities deployed by terrorists in past attacks and projections of potential future terrorist capabilities. This list largely already exists within the current DOE DBT and its supplementary Adversary Capabilities List (ACL).

2. **Assign relative resource point value scores to each capability.**
   The most difficult portion of the process, this step requires a group of experts to assign relative numerical values—in a generic "resource point" scale—to the various capabilities. These values would be assigned based upon the experts' opinions regarding the perceived difficulty for an adversary to do the following while avoiding pre-attack detection:
   - Acquire/develop the capability
   - Infiltrate the capability into the U.S. (or acquire it within the U.S.)
   - Train to use the capability
   - Stage the capability near the targeted facility (i.e., at a safe house)
   - Deploy the capability at the targeted facility in immediate preparation for the attack
3. **Analyze a range of past attacks to determine the "total resource point value" of each attack.**
   With the list of all potential adversary capabilities, an analysis can be conducted of a set of historical terrorist attacks to determine the total resource point value of each attack (i.e., the "sophistication" level of the attack based on the capabilities the attackers deployed).
4. **Assign a "resource point cap" for each DOE/NNSA facility, such that the attack scenarios they analyze their security against have adversary capabilities that sum to less than the assigned cap.**
   Based upon the analysis of historical terrorist attacks, projections of future threats, and risk management considerations, DOE would assign a resource point cap to each facility. Facility security managers would use this cap as the basis for constructing their security analysis scenarios. The individual resource point values for each of the adversary capabilities used in a single attack scenario must sum to approximately (but not greater than) the assigned cap.

EXAMPLE IMPLEMENTATION AND APPLICATION

The steps listed above can be followed through with a small fictitious dataset to illustrate the proposed approach. First, a list of potential capabilities an adversary might deploy is created. The list is populated with capabilities terrorists have utilized in past attacks, and projections of capabilities they may deploy in the future. Table 1 shows a small example of such a list.

Table 1. Example Resource List

Personnel and Training
Elite-trained infantry weapons operator
Basic-trained infantry weapons operator
Elite-trained explosives operator
Basic-trained explosives operator
Small airplane (fixed-wing) pilot
Helicopter (rotor-wing) pilot
Suicide bomber

Explosives
Large bulk charge
Medium bulk charge
Small bulk charge

Vehicles
Helicopter
Small airplane
Large truck
Car / SUV

Weapons
5.56mm assault rifle
7.62mm assault rifle
7.62mm machine gun
Rocket Propelled Grenade
.50-caliber sniper rifle

The level of detail in this list would be driven by a variety of factors. For instance, the small list shown in Table 1 delineates a difference between types of personnel based upon their areas of expertise (explosives, infantry weapons, pilot, etc.). At a more granular level, it also differentiates between "elite-trained" personnel of certain skill types and "basic-trained" personnel of the same skill type.

Once the resource list is compiled it must be populated with resource point values. The values require expert consensus on what an appropriate relative "sophistication" is for each resource, based on the criteria listed in the section above. Some difficulty is expected during this expert deliberation and discussion process: assigning quantitative values to qualitative opinions is always difficult, particularly, in this case when assigning such values on a general and relative scale that must be the same for disparate capabilities. Well known expert elicitation techniques can ease this process.

To continue the illustration of the example, Table 2 below shows the earlier example resource list populated with somewhat arbitrary values selected by the author.

Table 2. Example Resource List with Resource Point Values

Personnel and Training	**Points**	**Requirements**
Elite-trained infantry weapons operator	20	One per team required for multiple coordinated attacks
Basic-trained infantry weapons operator	5	
Elite-trained explosives operator	25	
Basic-trained explosives operator	10	
Small airplane (fixed-wing) pilot	15	
Helicopter (rotor-wing) pilot	20	
Suicide bomber	5	

Explosives		
Large bulk charge	40	Requires at least one elite-trained explosives operator
Medium bulk charge	25	Requires at least one basic-trained explosives operator
Small bulk charge	2	

Weapons		
5.56mm assault rifle	2	
7.62mm assault rifle	2	
7.62mm machine gun	15	
Rocket Propelled Grenade (RPG)	5	
.50-caliber sniper rifle	10	User must be elite-level trained

Vehicles		
Helicopter	40	Requires at least one helicopter pilot
Small airplane	35	Requires at least one fixed-wing airplane pilot
Large truck	5	
Car / SUV	4	

Based on this completed resource point list, historical terrorist attacks can be analyzed to determine the total resource points "used" by the attackers to gain a better understanding of how "sophisticated" the attack was in terms of resources used. For instance, if a particular past attack

had the following description, the total resource points used for the attack would be determined as shown in Table 3:

> *Example Historical Attack: A suicide bomber drives a large truck with a medium-sized bulk explosives charge (i.e., a VBIED), into a federal facility and detonates.*

Table 3. Total Resource Points Computation for Example Historical Attack

Resource	Quantity	Item Point Value	Line Point Value
Suicide bomber	1	5	5
Large truck	1	5	5
Medium bulk charge	1	25	25
Basic-trained explosives operator	1	10	10
		TOTAL:	**45**

Note that a "basic-trained explosives operator" is included in the computation, despite the fact that it was not explicitly stated in the scenario description. This is because the resource list in Table 2 stipulated a requirement that to use a medium-size bulk explosives charge, at least a basic-trained explosives operator was required to build the device. The requirements placed on the use of resources by the experts who develop the table will influence the scenario: in this case the explosives charge is considered large enough and complex enough that some basic explosives training is required to construct the bomb.

By analyzing many historical attacks in this way, trends can be assessed and outliers identified. From a plot like that shown in Figure 1, DOE can better identify what resource point caps it should apply to its facilities.

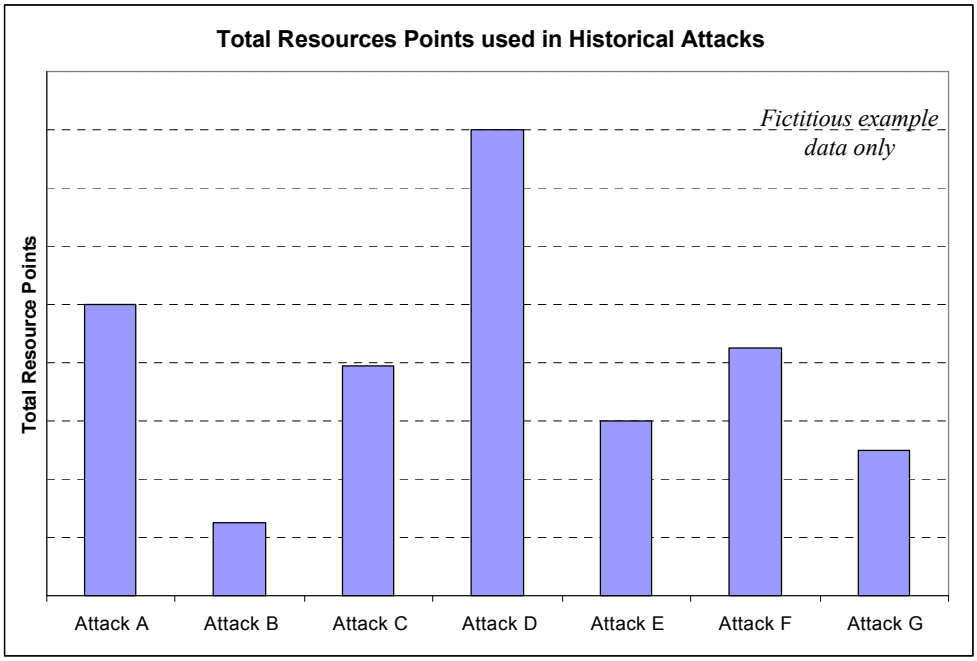

Figure 1. Example Plot Analyzing Historical Attacks

To conclude our simple example of the resource point-based DBT in operation, we assume DOE has selected a resource point cap of 100 points for a particular facility. Using this 100 point cap, and the example resource list and values in Table 2, two different scenarios can be constructed for attacking a secure target building at the facility in a sabotage attack:

Scenario 1: Helicopter drops four-person adversary assault team equipped with 7.62mm assault rifles and small bulk satchel charges used to explosively breach the building and sabotage the target.

Table 4. Hypothetical Example Scenario 1 Resource List

Resource	Quantity	Item Point Value	Line Point Value
Helicopter	1	40	40
Helicopter pilot	1	20	20
Basic-trained infantry weapons operator	3	5	15
Basic-trained explosives operator	1	10	10
7.62mm assault rifle	4	2	8
Small bulk charge	2	2	4
		TOTAL:	**97**

Scenario 2: A single suicide bomber explodes a medium-size truck bomb at the facility perimeter to breach the fence, after which an assault team of six adversaries in two SUVs attempts to enter the perimeter, reach the building, explosively breach the building, and sabotage the target. Each member of the assault team is armed with a 7.62mm assault rifle.

Table 5. Hypothetical Example Scenario 2 Resource List

Resource	Quantity	Item Point Value	Line Point Value
Large truck	1	5	5
Medium bulk charge	1	25	25
Suicide bomber	1	5	5
Basic-trained infantry weapons operator	6	5	30
7.62mm assault rifle	6	2	12
SUV	2	4	8
Basic-trained explosives operator	1	10	10
Small bulk charge	2	2	4
		TOTAL:	**99**

Note that both scenarios are constructed such that the resources used approach the 100 point cap, but do not exceed it.

POTENTIAL ADVANTAGES OF A RESOURCE POINT-BASED DBT

The fundamental purpose of the resource point-based DBT concept is to better align DOE threat policy with trends seen in historical terrorist attacks and projections of potential future terrorist capabilities. Also, it is intended to provide better definition of the threats DOE facilities are expected to defend against and serve as a tool for consistent communication of adversary threat scenarios across the complex and to key decision makers. In striving to achieve these goals, the proposed resource point-based DBT concept may offer several potential advantages over the current DBT policy. These include:

- The proposed resource point-based DBT method restricts the number of very advanced capabilities available to attackers in a single security analysis scenario, and curtails the use of a very large adversary force in combination with multiple very sophisticated capabilities.
- The resource point-based method allows and encourages security analysts to analyze the impacts of an adversary's use of single very advanced capabilities, but restricts such scenarios by limiting such an adversary's ability to deploy other capabilities. Importantly, it enables the potential adversary use of single advanced capabilities to be factored into the overall determination of security system effectiveness and total security risk.
- The proposed DBT method better accounts for the difficulty of an adversary obtaining and fielding advanced capabilities within the hostile operational environment of the United States. The possibility of pre-attack detection is factored into the resource point values assigned to the various capabilities.
- The proposed method enables DOE/NNSA facilities to analyze their security against attacks with a wide range of number of attackers, but with a trade-off in number of attackers and other capabilities. It is possible that the method will enable DOE/NNSA facilities to analyze their security effectiveness against extremely large adversary forces—as called for by Government Accountability Office (GAO) findings [1].
- The resource point-based method continues allow DOE to use a "graded approach" to threat assignment; and likely enables even greater granularity in the graded approach by allowing different resource point caps to be assigned to individual facilities.

CONCLUSION

The proposed resource point-based concept is but one possible approach to reforming the DOE DBT. It attempts to better ground the DOE security analysis scenarios in the combinations of capabilities and personnel numbers seen in actual terrorist attacks—with careful assumptions of the future. Critically, the method allows adversaries to use a single very advanced capability, but at a significant operational cost, and enables their use to be incorporated into final determination of security system effectiveness and total security risk. Finally, the method also accounts for the possibility of pre-attack detection inherent in more sophisticated attack scenarios.

FUTURE WORK

An extension of the resource point-based DBT concept—and integration with other potential reforms to the DOE security/vulnerability assessment methodology—has been proposed by Sandia National Laboratories' Security Systems and Technology Center [2]. This work will use

the resource-point concept as a basis for creating risk-based cost-benefit optimization tools for making security planning decisions at both the facility- and complex-wide levels, as well as explore the application of belief/plausibility uncertainty methods to better capture the highly uncertain nature of qualitative expert opinion inherent in creating a postulated threat policy like the DBT [3].

REFERENCES

[1] Nazzaro, Robin M., DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat, Testimony before the Subcommittee on National Security, Emerging Threats, and International Relations; Committee on Government Reform; House of Representatives, U.S. General Accounting Office, April 27, 2004.

[2] Wyss, Gregory D. et al, "Risk-Based Cost-Benefit Analysis Tool", FY2009 LDRD Proposal, Sandia National Laboratories, May 2008.

[3] Darby, J., 2007, "Evaluation of Risk for Acts of Terrorism using Belief and Fuzzy Sets", Journal of Nuclear Materials Management, Vol XXXV, Number 2, Winter, 2007